Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Health telematics networks

Julia, Rosa; Poullet, Yves

Published in:
The EDI Law Review

Publication date:
1997

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (HARVARD):
Julia, R & Poullet, Y 1997, 'Health telematics networks: reflections on legislative and contractual models providing security solutions', *The EDI Law Review*, vol. 4, no. 3, pp. 177-203.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 05. May. 2023

The EDI Law Review **4**: 177–203, 1997.
© 1997 *Kluwer Law International. Printed in the Netherlands.*

Health Telematics Networks: Reflections on Legislative and Contractual Models Providing Security Solutions

YVES POULLET & ROSA JULIA-BARCELO
Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium

Abstract. Health telematics enables medical services to be carried out in an electronic way. From a legal point of view such activity raises several issues, specifically in privacy and security matters: Health electronic records and messages have to ensure authenticity, integrity and confidentiality. These privacy and security requirements can be fulfilled by employing electronic signatures, trusted third parties' services, and cryptography. Consortia of health care professionals willing to adopt such technical solutions will need to enter contracts with the providers of security services, specifically, with the providers of registration and certification services, providers of value-added services, network providers and, finally, between themselves. These contracts will govern the use of such services and will create a set of duties and obligations to be fulfilled by those wishing to participate in such secure networks. Therefore, this article endeavours to provide suggestions regarding these contracts to be adopted by health care actors. In addition, because such services have not yet been regulated, the paper points out some necessary new legislation.

Key words: contracts, digital signature, certification authority, national professional organisations, value-added services, liability.

1. Introduction

During the last decade the use of telematics in the health care sector has become more and more widespread. The use of information technology and telecommunications in the provision of medical services enables, *inter alia*, the following types of services to be carried out through networks: consultation of medical databases, remote diagnosis and treatment, prescription of drugs, sending of referral or discharge letters between general practitioner and hospital specialist, sending requests and reports relating to laboratory investigations or radiological examinations (e.g., x-ray and magnetic resonance imaging). It will also allow patient records to be available to authorised health care professionals any time, anywhere over these networks.

In addition, medical laboratories, pharmacies and health insurance organisations are now able to communicate with each other by electronic means, providing the possibility to process electronically insurance claims, reimbursements, payments, etc. Moreover, hospitals engage in important business activities which can be carried out by electronic means. For instance, providers

of medical goods (e.g., medicines) may enter electronically supply contracts to fulfil hospitals' needs.[1]

As a result of the development of health telematics several advantages arise, including accuracy and completeness of patient records, easy access to patient information by health care workers, improvements in the quality of care, improvements in the productivity of health care workers, improvement of health institution management and documentation and collection of fees.[2]

In order to facilitate the communication of electronic messages a set of clinical EDI messages has already been designed and standardised to cover a range of exchanges between local family doctors and hospital/laboratory services.[3] This standardisation activity is currently under expansion by the European Board for Edifact Standards (EBES).[4] Working Party 4 (on facilitation of International Trade Procedures) of the Economic Commission for Europe of United Nations (UN/EC) acts as supervisor of these standardisation activities.

2. Legal Problems: Security and Privacy

As the above description reveals, a health telematic system is based on electronic communications, sometimes with a standardised format and often containing sensitive and personal data. For the reasons explained below, the health records exchanged by electronic means must have authenticity and integrity both with regard to their content and their originator and they must also to be kept confidential.[5]

The need to ensure authenticity and integrity arises for evidentiary purposes: if a trial occurs, the parties need to have the appropriate instruments to prove the author and content of the document (for example in a malpractice lawsuit). In addition, the requirements of written documents and signatures as tools providing authenticity and integrity sometimes exist as a matter of contract[6] or administrative law.[7] In other words, sometimes a written document with a hand-written signature must be produced to achieve the validity and enforcement of contracts or administrative acts. In the context of paper-based documents, the hand-written signature at the bottom of a written document is used to prove the author of the document and its integrity, i.e., it proves who is the real author and that the document has not been changed. In the electronic context, digital signatures and trusted third parties' services ensure the fulfilment of the same legal requirements.

Also, as a matter of evidence, health electronic records sometimes need to show the time they were produced, sent and (often more importantly) received. For instance, a specialist might want to prove he sent a statement and that he did it at a specific time. While in a paper document scenario this can be achieved through postal services (e.g., acknowledgement of reception), in a health telematics scenario it is necessary to discover appropriate ways to provide such services.[8]

With respect to confidentiality, the exchange and storage of electronic medical data must comply with the legal requirements provided for in the European Directive on the "protection of individuals with regard to the processing of personal data and on the free movement of such data" adopted on 24th of July 1995. While in a paper-based scenario this was achieved through physical mail and archiving services (e.g., envelopes, registration, courier services), in a health telematic situation this could be achieved through the use of cryptography methods, as described below.

Acknowledging the importance of providing an adequate legal framework ensuring the security and confidentiality of electronic medical records and exchanges, the Council of Europe adopted the Recommendation N° R (97) 5 on medical data on the 13th of February 1997, article 9 of which deals with security problems. Indeed, article 9.2 establishes that appropriate measures should be adopted in order to protect the integrity, authenticity and privacy of medical data.[9]

3. Description of a Secure Health Care System

The need for security measures, both for authenticity and integrity purposes and for privacy ones, brings onto the scene new actors who will take charge of providing such services. In the following discussion, we describe, first, the actors involved in a health telematic network, specifically those conducting security functions, and second, how technical tools, specifically digital signatures and trusted third parties' services will fulfil the requisite security functions and how cryptographic methods will provide us with solutions for privacy issues.

3.1. *Overview of the Actors Involved in a Health Telematic Network, Functions and Contractual Relationships Between Them*

As we will explain with more detail below, in a secure health care network, we distinguish between three kind of actors:

1. Actors who send and receive electronic messages in order to carry out activities related to medical services: doctors, medical laboratories, pharmacies and health insurance organisations, providers of medical goods, etc. Notice that patients are not included among these actors.
2. Actors involved in functions directly related to the functioning of the health telematic network: (1) Trusted third parties conducting registra-

tion and certification services in order to make operable digital signatures and (2) Trusted third parties or value-added services for securing communications.

3. Network providers: By definition a heath care telematic network needs a network provider. To communicate data electronically through a network, generally direct communication can be made via public data networks or private leased lines or by signing up to the services of a third party network provider (known as value-added network service providers), which is the predominant tendency. This latter method offers a range of services such as message handling and translation as well as consultancy, project management and could also provide notarial services described below. Currently network providers have interconnections with other network providers.

Concerning relationships between the actors, the need for security in communications requires several functions to be carried out (registration-certification functions, secure communications, privacy functions). The actors in charge of providing such services will need to enter contracts with the actors of the health care systems (hereinafter "subscribers"). This will lead to the following relationships:

1. Contracts between the users and the Trusted third parties, specifically with the registration-certification authority.
2. Contracts between the users and the value-added services.
3. Because the use of a health telematics system technically requires a network service provider, each actor in a health care telematic system (e.g., a hospital) will be required to enter a "network agreement contract" with the provider.[10]
4. Finally, the actors in charge of carrying out medical services should enter previous agreements between them establishing the legal terms, and technical conditions, under which parties conducting electronic communications will operate. In doing so, several EDI Model Agreements may be taken into account.

Therefore, it is clear that a complicated legal framework, with different contracts linking the various actors, must be established. Below we will endeavour to provide recommendations for contractual provisions to be adopted between the actors involved in a secure health telematic network. We will also point out several areas where reforms of law would be appropriate.

3.2. *Description of Cryptographic Techniques: Digital Signatures and Registration-Certification Functions for Authentication and Integrity Purposes*

Nowadays, mathematicians ensure that the most reliable technical security solution for secure user identification and integrity of content is the digital signature, based on asymmetric public key encryption with a hash function.

Asymmetric public key encryption systems use a key (private key) to encrypt and a different, but mathematically related, public key to decrypt messages. The key is a sequence of symbols that determines the transformation form unencrypted plain text to encrypted ciphertext, and vice-versa. The security of digital signatures lies in the authenticity of the public key: the link between the key and the key-holder (this public key belong to the sender) should be ensured as well as that the private key has not been disclosed (see below the function of the registration and certification authorities as well as public databases containing public keys non revoked).

Using asymmetric public key encryption, a user can apply his public key to a message, sending the transformed version together with the original message to the intended receiver. The receiver would verify the message by applying the sender's public key (obtained from a public database, see below) to the encrypted message and seeing that the result matched the original message.

Therefore, because a particular public key can only decrypt messages encrypted using the mathematically related private key, one who receives a message (a ciphertext) signed by the sender's private key and successfully verifies it using the mathematically related public key (by applying the public key to the encrypted message and obtaining the message in plain text) can be confident, first, that the author of the message is the key holder of the related private key (except in cases of compromise, see below), and second, that the content of the message received is the same as the one that was sent. Thus, the use of asymmetric public key encryption permits authentication of the sender's identity and assures the integrity of the message.

In practice, the private key is applied to sign shorter "message digests" rather than entire messages. In most digital signatures based on public key techniques,[11] a one-way hash function is used to produce a condensed version of the message, to which is applied the sender's private key. The condensed signed version, along with the entire message to which the one-way hash function has not been applied, is sent to the recipient. When it is received, the message digest cannot be reversed to obtain the message because the hashing method is a one-way function; thus the receiver, after verifying the signature, also processes the entire, uncondensed text with the hashing algorithm, and compares the resulting message digest with the one the sender signed and

sent along with the message. If the message was altered in any way during transit, the digests will be different, thus revealing the alteration.[12]

As noted above, the trustworthiness of digital signatures lies in the reliability of the keys: The keys must give satisfaction that the party with whom one is communicating is exactly the one he is believed to be. According to standard X509 v3, this can be achieved through the establishment of independent "Trusted third parties" ("TTP's"), who provide the requisite assurances of identity by binding public keys to the identity of their owners through the issuing of certificates.[13]

The certificate contains identifiers such as the following: a) the name by which the subscriber is generally known; b) the distinguished name of the subscriber;[14] c) a public key corresponding to a private key held by the subscriber; d) the serial number of the certificate, which must be unique among the certificates issued; e) the date and time on which the certificate was issued and accepted; f) the date and time on which the certificate expires;[15] g) the distinguished names and addresses of the certification authority issuing the certificate; h) the recommended reliance limit for the certificate.

Apart from this identification function, in a health care context another equally important function of certificates is the certification of professional status. Therefore certificates should contain also other attributes such as membership of a chamber of physicians or the like.[16]

The process of issuing a certificate contains several steps: (1) the registration function, i.e., ascertaining the identity of the key holder who subscribes to the registration and certification services;[17] (2) name assignment, i.e., the function of assigning individuals and companies (e.g., health care institutions) unique names and addresses; (3) the certification function. After a successful completion of the registration and naming procedures by the registration authority, the certification authority[18] can issue the certificate as follows: A one-way hash function is applied to the information contained in a certificate (see above) and then is signed using the certification authority's private key. This signature is attached to the same information, non-encrypted, in order to form the certificate. Therefore, the certificate has two parts: the information non-encrypted (to which the hash function has not been applied) and the digital signature itself. The certificate binds party A (or A's name) with his public key. The certification authority frequently not only issues the certificate but also creates the key.[19] However, often the registration function and the certification function are carried out by different entities.[20]

To use the certificate, every time that the sender A enters into communication with the receiver B by sending him a message encrypted using A's private key, he should send along with the message the certification authority-issued certificate. This will allow the receiver B to ensure himself that the sender

is actually the sender A, as well as his attributes (e.g., A is a nurse). He does so as follows: party B cannot verify the message without access to party A's public key listed in the certificate, which he receives together with the message. Because the certificate contains party A's public key, signed by the certification authority's private key, and because the certification authority's public key will always be publicly available on a database, maintained by the certification authority, party B can use the certification authority's public key to verify the certificate sent along with the message by party A and if party B does it successfully, party B will have party A's public key. Having thus verified the signature of the certificate, party B can verify the message.

The certification authority has the obligation to constitute and maintain a directory or data base, accessible on line, containing a list of all the certificates issued and those which have been revoked. Once notified of a key compromise, a certification authority should have a duty to publish this in the certificate data base within a determined (short) period of time. Therefore, a receiver of a certificate may check in the database whether the certificate is valid or whether it has been revoked.

3.3. *Description of Value-Added Services for Securing Communications*

For a health telematic system to function properly, the actors must be confident not only that the messages sent were actually sent by the person they purport to have been sent by (which as we have seen above is achieved though TTP-registration and certification services), but also other functions need to be ensured:

1. Proof of receipt of the messages: because the sender must be able to demonstrate that his own messages were actually received, a function of providing proof of the reception of the message by the participant to the network should be provided. For example, if a health care actor uses a valued-added network, upon reception of the message by the value-added network mailbox, the value-added network should send to the sender a digitally signed confirmation message of the receipt by the intended receiver (because the value-added network put the message in the intended receiver's mailbox) (see below).[21]
2. Time stamping: the function of providing the exact time of the message or a hash function of this message handled by the participant to the network.[22]
3. Storage of messages: the function of keeping a copy of a message in order to certify at the request of one of the participants to the communication the existence and the real time of the reception and sending of the message by the network information system.

4. Arbitration: in case of dispute between the communicating parties about the existence or reception time of a message, the TTP can be authorised by the two parties to establish the exact nature and content of the message stored by it.
5. These functions can be achieved thorough TTP services called value-added services or "*notary services*" (offering proof of activities between the communicating parties).[23]

3.4. *Analysis of Cryptography Methods for Ensuring Privacy Requirements*

Symmetric encryption has played an essential role in protecting the privacy of messages and electronically stored information. This technique uses a key to encrypt messages and the same key is used to decrypt messages. In fact, the use of cryptographic methods for the protection of confidentiality has been foreseen by the Guidelines on Cryptography Policy issued by the OECD last April.[24]

In addition, the use of encryption for confidentiality may employ a combination of symmetric cryptographic systems for encrypting data and asymmetric systems for managing the keys.[25] This works as follows: First, the sender A will generate a session key, that is a symmetric key generated for use only once for security reasons. Second, with the public key method, the sender A will directly encrypt the session key with the public key of the recipient B. A does so as follows: he encrypts his message *twice*, once with his own private key, and again with B's public key. When B receives this message, he must decrypt it twice, once using A's public key, and again using his own *private key*. Because nobody else will have access to party B's private key, nobody else will be able to decrypt party A's message even if they are able to hijack it from the network. Third, A signs the message with his private key and encrypts the plain text with the session key and sends both together. Fourth, when the receiver receives the message, first he will decrypt the message using the session key in order to get the plain text. Then, he will verify the signature.

Concerning cryptography regulation, European policy makers should adopt solutions in accordance with European privacy laws. Privacy solutions where the main key is deposited with government (key escrow) are uncertain to comply with the privacy laws.[26]

4. Recommendations Regarding Security Functions

4.1. *Trusted Third Parties Conducting Registration and Certification Services*

As we have seen above, the use of Trusted Third Parties carrying out certification services is required to make digital signatures operable. At present these services are offered to users by private companies developing activities in the field of computer security under contractual arrangements.

Until now, in Europe there has been no legal regulation of Trusted Third Party services despite several projects or recommendations: among others, we note the following: Green paper on the Security of Information Systems of 1994, which was never published as an official paper; the German Draft Digital Signature Law (version of September 19, 1996), the UK government paper on the provision of encryption services to safeguard integrity and confidentiality (10th June 96); the Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of Cabinet Bangemann and Monti entitled "A European Initiative in Electronic Commerce" announcing EU legislation on digital signatures and "digital certificates" (12.04.97).[27] On a broader level, note the following: the Recommendation of the OECD entitled "Guidelines for cryptography policy" (27 March 1997);[28] the preparatory works of the UNCITRAL about electronic commerce and specifically about trusted third parties (see Vienna 12–30 May 1997).[29] Finally, in United States, many states have drafted legislation,[30] we have to point out several federal initiatives such as the electronic communications certifying system of the U.S. Postal Service, and the American Bar Association Guidelines for Digital Signatures which provides a framework for standardised digital signatures.[31]

In our view, for the following reasons, enacting new legislation in Europe will enhance the use of health telematics: (I) because offering security services under legal requirements would offer more reliability in certification authority practices; (II) because giving TTP's predictable obligations (rights and duties) would provide clarity; (III) because the establishment of objective criteria for becoming a TTP will help avoid situations of monopoly which could be enhanced by attributing this function to a special body and (VI) because defining a legal framework would help achieve a proper balance between the liability of TTP's and users.

In the following paragraphs, we will try to provide some suggestions that should be taken into account if TTP legislation is to be enacted:

a. *Principles to be respected by the TTP's developing registration and certification services*. In our view the law regulating TTP's should respect three major principles:

a) Neutrality. The main requirement for a TTP, specifically for a certification authority, is to be impartial and independent in order to inspire trust, first to the users, finally to the court which might have to value (in a lawsuit) the electronic document signed using digital signatures.
b) Free choice of the trusted third party. There should be no obligation or external pressure (including by professional associations) to join a specific telematic network; the market should provide different options and the users should be free to choose the one they find best.
c) Interoperability of TTP services. The law should ensure TTP's follow standards in order to interoperarate with other TTP's. Also, the law should require an agreement between TTP's ensuring the principle of mutual recognition and their acceptance of common administrative and technical standards in order to facilitate exchanges between electronic communicators, notwithstanding their reliance on the services of different TTP's.

b. *Conditions for becoming a TTP developing registration and certification services*. As provided by most of the recommendations and draft law regulating TTP services, the main conditions for becoming a TTP should be the following ones:
   a) Control of the financial means of the TTP in order to cover their eventual liability. The proof thereof is provided by showing a "suitable bank or insurance company guaranty";
   b) Proof of their rights to hardware and software (especially use of cryptography licences).
   c) Quality and accountability of the employees involved.
   d) Compliance with the legal requirements provided for in the European directive on the "protection of individuals with regard to the processing of personal data and on the free movement of such data" adopted on 24th of July 1995.

c. *Responsibility of TTP's developing registration and certification services*. The extent of responsibility of TTP's is uncertain: recognising this fact, principle 7 of OECD's Guidelines for Cryptography Policy says "Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold access to cryptographic keys should be clearly stated". The existing TTP's disclaim or limit to the amount the subscriber paid for the certificate any responsibility for anything it says, therefore undermining the reliance on the certificates by users and, in our view, largely defeating the purpose of having a certificate. Until this question is resolved it risks inhibiting the spread of health telematics and electronic commerce in general because of the lack of confidence it causes in digital signatures and certificates. In the following discussion we provide recommendations to the policy makers or eventually to the drafters of contractual clauses to be inserted in contractual arrangements with TTP services (registration and certification).

The law (or a contract) should define the obligations of the registration authority and certification authority (basically ascertaining identity/status and certifying identity, status and others), defining the level of inquiries to be carried out in order to make the statements in the certificate. Also, it should establish the level of care the registration and certification authority should bear in carrying out these obligations.

Among the different criteria of responsibility (strict liability, duty of care, none), in our view, it is important to keep an appropriate balance between the certified parties, those who rely on certificates and the registration /certification authority, and the TTP's, in order to enhance health telematics, and electronic commerce in general. For example, a law which allocates a very high standard of care to the certification authority would discourage any organisation from undertaking such business activity or will force them to raise prices in order to pay for insurance cover.[32] On the other hand, if the certification authority is not liable because the standard of care is very low (not responsible even if he negligently misidentifies the key holder), this will not provide enough trust, and accordingly, users might prefer to use paper documents and hand-written signatures, and ultimately, the courts will not grant value to electronic documents signed digitally.

In our view, because the functions of the registration and certification authority are different and they may be carried out by different entities (although they could be conducted by the same actor), also as a matter of liability a distinction should be made between (1) liability of registration authorities and (2) liability of certification authorities.

Concerning the liability of the registration authority, it should be required to act with reasonable care in ascertaining the critical facts about the subscriber's identity. Accordingly, if the registration authority fails properly to identify the subscriber, it should be responsible under the criteria of "reasonable care". More important, the relying person who suffers a loss as a result of a fraudulent certificate (e.g., because a registration authority misidentifies the key holder who uses the certificate in a way that harms the relying person) and who has no contractual relationship with the registration authority, should be able to claim against the registration authority for liability arising from tort. In such cases, the liability of the registration authority will depend on the standard of care defined by the representations it makes in the certificate about the level of inquiry it promises to make before issuing a certificate.

Concerning liability of the certification authority, it should be responsible in the event it fails to bind a public key to the right owner (or for instance, fails to discover the insufficient key length of the public key holder or uses itself an insufficient key length to sign certificates). Nevertheless, by adopting the criteria of "duty of care" the key holder would bear the burden of demonstrating the lack of care, and given the very specialised technological aspects involved in issuing a certificate, this burden would be exceedingly difficult to meet. Therefore, in our opinion the burden of proof should be reversed; the certification authority should have to prove its lack of negligence by showing that it fulfilled a set of standardised rules for issuing the certificate.

Also, as discussed above, the TTP acting as certification authority has the obligation to constitute and maintain a directory or data base, accessible on line, containing a list of all the certificates issued and those which have been revoked. Therefore, the TTP-certification authority should assume responsibility for the accuracy, updating and completeness of its directories *vis-à-vis* both its own subscribers and third parties which suffer damages when relying on wrongful issuance or non-issuance of a certificate. Additionally, the subscribers should engage to give notice to the certification authority in a short period of time of revocations or changes in their status. They may be held responsible if they do not do so. In our view, if a digital signature is used by an unauthorised person, it should be sufficient for the certificate holder to assert that a message was signed without his authorisation and it should be up to the certification authority, as is regulated in bank card fraud losses,[33] to prove that the key-holder did not give notice of the key compromise before the fraud was performed, which means that the *onus probandi* is reversed.[34] It is important to notice that the provision of information to the certification authority is the event that will transfer the risk of loss from the key holder to the certification authority.[35]

In fact UNCITRAL has proposed a similar regime to the one just described by adopting the criteria of "duty of care" as well as a presumption of responsibility on the part of the certification authority that could be rebutted by the certification authority proving compliance with a set of rules and requirements (code of conduct) established by law or by contract.[36]

Finally, the law should require that specific insurance must be taken by the certification authority in order to cover their civil liabilities as specifically required by the Utah Law (46-3-310).

d. *Privacy requirements to be fulfilled.* With respect to the nominative data processed by the registration authority concerning health professionals, it is quite clear that this processing must be justified by an explicit consent of the subscriber. That means that each subscriber must be informed of the purposes of this processing. The right of access is exercised easily by consulting the register.

4.1.1. *Possible Role of National Professional Organisations (Such as Chambers of Physicians)*

As explained above, digital signatures offer authenticity and integrity of documents if they are employed with Trusted third parties, who ensure the identity of the subscriber by binding public keys to their owners through the issuing of certificates. Before issuing a certificate, the Trusted third party must obtain appropriate identification documents demonstrating the certificate requester's identity.

Moreover, in a health telematics framework, certificate requesters wishing to operate as actors in a health telematics system need to demonstrate to the registration authority not only their identity but also their professional status and in which quality they would like to participate in health telematics services.

National professional organisations (such as chambers of physicians) will of course continue to be responsible for the authorisation of different categories of health care professionals. Accordingly, such an organisation should issue under request of the health care practitioner statements certifying the deontological and legal competence of the requester to provide health care services. The certified party can then submit this statement (called professional certificate) to the Trusted Third Party (first to the registration authority and then to the certification authority) in support of his digital certificate request. This certificate of professional status to be provided to the TTP (registration authority) could be issued in electronic form, and in such a case it should be signed electronically with the private key of the chamber of physicians or other professional association. It could prove necessary to confer by law this responsibility on the chamber of physicians or other professional association. Also, in the countries where no such official professional association exists it will be necessary to determine which authority will carry out this function (e.g., there is no national organisation for certifying the status of nurses). In addition, EU harmonisation for health telematic purposes of the concept of different categories of practitioners will be necessary.

Therefore, from what it has been said above, the procedure a physician should follow to obtain a certificate would be as follows: 1. Request to the chamber of physicians of a statement certifying the professional status; 2. Submission of this statement as well as other identification documentation to the registration authority; 3. Upon presentation of these documents, the certification authority will issue a certificate.

Health care practitioners may also wish to include in a certificate the exact status, quality, and period of time in which they have acted in a specific health care institution (e.g., N.Y. Hospital). For doing so, the employer could emit paper or digital statements that should be submitted to the registration authority in order to be included in the certificate.

4.2. *Providers of TTP Value-Added Services for Securing Communications*

At present, value-added services as described above are provided by value-added network providers only under contractual bases, without any legal regulation. In the following discussion, we will endeavour to provide some recommendations to be taken into account when drafting contracts between the providers of value-added services and the subscribers of such services. Alternatively, it should be considered whether it would be positive to undertake legal regulation of those services.

As should the TTP-registration-certification authorities, and for the same reasons, the providers of value-added services should be subject to the criteria of neutrality, free choice and interoperability.

It would exceed the scope of this article to deal with all possible value-added services to be offered. Let us examine only one of them, the proof of receipt. By offering the service of providing proof of receipt, as explained before, the value-added service provider should engage itself to guarantee the messages were routed to their intended destination and confirm the delivery of the message.[37] The confirmations come to the sender signed by the value-added service (if the intended receiver fails to send on his own an acknowledgement of receipt, see below). By obtaining such proofs of receipt, in case of a lawsuit, the sender could show not only that he sent the message (because of the confirmation signed by the notarial service) but also its content.

The law could provide that the provision by a value-added service provider of an acknowledgement of receipt establishes a presumption that the receiver received the message as indicated by the acknowledgement.[38] One can imagine a law governing such service similar to the rules regulating the Post Office activities regarding acknowledgement of receipt.

Among the existing value-added services (see above), it will be useful to define by the health care actors which value-added service should be subscribed by them. In particular, concerning the proof of receipt it should be defined when to use this service. For example, proof of receipt may be provided depending on (1) the nature of the different kinds of messages (e.g., is it of vital interest for a patient?); or (2) whether the receiving party has not by itself sent the acknowledgement of receipt as he is required to according to the interchange agreement (see below).[39]

Concerns regarding privacy issues arise when value-added services are provided: with respect to the storage of messages, processing, routing, time stamping, etc. These different legitimate purposes of the value-added services must be explicitly specified *vis-à-vis* the user and a right of access to the nominative data stored must be granted to him.

4.3. *Recommendations for Network Providers*

A health care telematics system needs a network or carrier, and this is likely to be provided by a value-added network service provider who will lease lines from a telecommunication company to connect up various nodes in their infrastructures. In this connection, two basic issues need to be considered: (1) what legislation should be enacted to govern the operations and responsibility of network providers, and (2) which provisions should be included in contracts between network providers (or value-added network service providers) and their customers. In many, perhaps most, situations, standard-form contracts will be used, and customers will not have the bargaining power (or ability) to negotiate specific terms. Therefore, it will be necessary for the law to provide appropriate protections for customers. In some cases, however, the larger health care actors (e.g., hospitals and laboratories) may be in a position to negotiate specific terms of their contracts with network providers. In these situations, the health care actors should consider the following recommendations.

4.3.1. *Concerning Liability Issues*

Firstly, it is necessary to identify cases in which network providers might be held liable. They include in particular the following:

1. Breach of confidentiality through a non-authorised access to the network (due to a lack of security in the transmission).
2. Corruption in transmission (wrong recipient, modification of the content, etc.).
3. Inadvertent or fraudulent loss of the message.
4. Delay in the transmission of the message.

In order to determine the consequences of any errors in terms of loss or alteration of the data or of breach of confidentiality, a specific assessment of the different potential risks for each kind of medical message should be developed by the consortia of health professionals. In relation to these different sources of damages, apart from the problem of locating the damaging acts and determining whether there has been a case of *force majeure*, it is recommended that health care actors insist upon network providers accepting a limited liability *vis-à-vis* their customers instead of excluding any liability. These limitations of responsibility will of course be available *vis-à-vis* the

contracting parties (e.g., hospitals) (except perhaps in cases of gross negligence), but not *vis-à-vis* third parties like patients suffering damages which are a direct consequence of the network provider's fault and who look for a remedy based in tort.

In our view, legislation should be adopted requiring the network provider to reverse the *onus probandi*, that is to say to prove the fault of the health care actors' system (e.g., by showing that the message received at the entrance of the information system of the network provider was already erroneous) or showing that it has been a case of force majeur.[41] Until such legislation is adopted, those health care actors in a position to do so should insist upon contractual provisions placing this burden of proof upon the network provider.

In cases of intervention of different network providers in transmitting a message, it would be more convenient for the user who suffers the damage to have a sole entity responsible for the entire network, more suitably the network provider directly in contact with him. This principle has been accepted by case law in the electronic funds transfer operations[42] and for similar reasons, it should adopted by law in the present case.

In any case, according to most privacy laws (e.g., the European Directive) each network provider has to provide adequate security measures. That includes notably: (1) nomination of a single individual to be responsible for data security and for facilitating the exercise of the access right; (2) maintenance of daily records of events related to data protection, this daily record shall be accessible to audit agencies; (3) maintenance of appropriate operational standards and reliable data security policies.

5. Recommendations for the Subscribers of Security Services

5.1. *In Their Relationships with the TTP's Providing Registration-Certification Services*

The contractual provisions of the agreement concluded between the subscribers and their Trusted third party providers of certification services have to contain certain obligations for the users, specific to the nature of the service. If these recommendations were adopted by policy makers when defining a legal framework for Trusted third party providers of certification services, it would not be necessary to adopt them on a contractual basis.[43]

1. The obligation to keep confidential the private key and to inform immediately the certification authority in case of "loss" or "theft".
2. The obligation to keep the certification authority informed as soon as possible of any modifications in their status as stated by the certificate issued by the certification authority.

Additionally, by accepting the certificate issued by a certification authority, the subscriber identified in the certificate certifies to all who justifiably rely on the information contained in the certificate that all representations made by the subscriber to the certification authority and material to information contained in the certificate are true.

5.2. *In Their Relationships with the TTP's Providing Value-Added Services for Securing Communications*

The agreements concluded between subscribers and Trusted third parties that provide notarial services must contain certain obligations for the subscribers, which at the same time, should be combined with the obligations assumed by the contracts governing the relationships between the health care actors themselves.

Concerning the only value-added service analysed herein (providing acknowledgement of receipt), contracts should include a provision with the following content:

In case of lack of reception of acknowledgement of receipt, the sender should send the message to the Trusted third party value-added service who will guarantee the message has been routed to the intended destination and he will sent to the sender an acknowledgement of receipt signed by him.

5.3. *Recommendations for the "Subscribers" of the Different Security Services in Their Relationships Between Themselves*

As noted above, it would be useful for the consortium of health care professionals to develop a common agreement available for all the transactions between subscribers. In such an agreement, the health care actors should establish the legal terms and the technical conditions under which they will operate electronically. The following should be among the legal provisions included: when the message should be deemed to be received; the evidential force of electronic messages and in particular the evidential value of Trusted third party value-added service acknowledgements of receipt (see above); security obligations; liability for errors, delays, etc. Among the technical conditions, health care actors should define the technical, procedural and organisational rules and specifications for the exchange of messages. The acceptance of this agreement would be considered as an essential element and condition for the participation in the secure health care network.

This agreement could be based on the model Electronic Data Interchange Agreement developed by the European Commission[44] or other Model agreements,[45] because most of the obligations foreseen by the model agreements

are adequate for regulating the communication of messages by health care professionals.

Thus, we suggest the basic following provisions:

a. *On the Reception of the Message*. The question arises about when the message should be deemed to be received: to the extent that the technology offers different choices of connections (direct leased lines, valued-added network mailboxes, etc.), the subscriber's agreement should contain a clause establishing when and where a message should be deemed to have been properly received.

For most of the EDI Model Agreements the "proper reception" of a message requires it to be accessible at a computer designated by the receiving party. For example, under the American Bar Association Model Agreement (art. 2.1.) a message is properly received when it is accessible to the receiving party at such party's designated computer. A similar approach has been taken by the European Model Agreement, which assumes that a message shall become effective upon receipt. Nevertheless, both the American Model (art. 2.2) and the European one (art. 5.2) foresee a clause by which parties could require an acknowledgement of receipt (in the American model it is an obligation). The European one states that if the acknowledgement is required and it is not received within a certain period, the sender is allowed to consider such a message as null. A similar approach has been taken recently by the UNCITRAL Model Law on Electronic Commerce (art. 14 and 15).

To the contrary, the German Basic EDI Model Agreement takes a different approach by providing that a message shall become effective not upon receipt of the message but upon receipt of the acknowledgement.[46] If the acknowledgement is not received, the sender is allowed to consider such a message as null. The Model foresees three different situations depending on the kind of network connection.[47]

Whatever contractual solution is adopted, it should be agreed that the reception by the sender of an acknowledgement signed digitally by the receiver will constitute conclusive evidence of the content of such a message. Therefore, the sender will be able to prove: (1) he sent the document; (2) the receiver did receive it; and (3) the content of the document itself.

In our opinion, where no acknowledgement is received, as we have seen above, the parties should agree to call a value-added service to act as intermediary (or notary) by providing a confirmation of delivery of the message. As we explained above, regardless of the existence of a law on the topic, the following clause should be included in the contracts entered between health care actors: upon proper receipt of any document, the receiving party should promptly transmit an acknowledgement of receipt signed digitally. When the

acknowledgement of receipt is not received, the sender should send again the message to the intended receiver and, after a specific period of time, require from the value-added network a signed confirmation that the message was routed by the value-added network to his intended destination (mailbox of the intended receiver). Therefore, it would be clear that the TTP-value-added service acknowledgement of receipt signed by him will constitute an evidence before court of the reception of the message by the addressee. Additionally, clauses specifying the timing for doing so should be included.

A similar approach has been foreseen by the Basic EDI Model Agreement, art. 8.3. *"If value added networks have been commissioned, a Message shall be deemed to have been received by the recipient if, by means of Data Transmission, the Message has entered the recipient's valued added network mailbox and a confirmation from that value added network has been received by the sender's Communications Equipment"*.

b. *On the Legal Validity and the Evidential Force of Electronically Interchanged Data*. Because the law sometimes requires documents to be in written form with hand-written signatures and because case law has not always taken a flexible approach about the concept of "written document" and "hand-written signature", it would be convenient for the parties to adopt a clause providing that neither party shall be entitled to assert the legal invalidity of messages for the sole reason that such messages have been processed electronically and have been transmitted, or retrieved, by electronic means.

On that point, we recall the principle of functional equivalent defended by UNCITRAL Model Law on Electronic Commerce (see art. 6 and 7): to the extent digital signatures used within digital certificates ensure at least the same authenticity and integrity (as we have demonstrated before) as hand-written signatures do, they must be regarded as valid signatures. Therefore, digital signatures (with certificates) should have the same force of evidence as "documentary evidence" and the parties should undertake not to contest the force of evidence of electronic documents and electronic signatures in the course of arbitration or judicial proceedings.[48]

c. *On the Need for Protecting the Confidentiality of the Messages*. Most of the European EDI Model Agreements contain clauses protecting the confidentiality of messages.

A health care telematics agreement should take the approach that all messages should be handled confidentially. Therefore, each party must ensure that the number of persons dealing with the processing of messages is restricted as far as possible and that all persons involved are obliged to observe security and confidentiality measures. Also, during the transmission of messages each

party must ensure the use of encryption methods for confidentiality. The same method can be used during the archiving of messages.

In producing, transmitting and archiving, each party must observe its own national regulations on data protection and employment law if messages contain personal data.

d. *On the Security Obligations and Checking of Malfunctions and Errors*. In general EDI Model agreements contain an obligation of using security procedures to ensure proper authorisation for transmissions and avoid improper access. Therefore, an agreement between health care subscribers should also contain a clause imposing the following obligation: (1) protection against unauthorised access and transmission, and (2) protection against loss of input and output of data after the data transmission.

Complying with such obligations will require, *inter alia*, the parties to carry out the security functions explained above.[49] Therefore, the parties should specify these security measures in an annex.

e. *On the Avoidance of Disruption, Malfunctions and Errors*. If one party detects a disruption in the communication system or if there is justified reason to presume such a disruption, that party should be obliged to inform the other party immediately. The obligation of information is found in most EDI model agreements.[50]

f. *On Liability*. The use of electronic methods for communication can produce mistakes and errors. If someone suffers loss or damage as a result of those mistakes, the question arises as to the liability of communicators: Inspired by the German Model Agreement the solution could be the following one:

Each party is liable for any damage arising from errors or disruptions within the party's *sphere of responsibility*. If in connection with a damaging event, any of the obligations concerning security measures stipulated in (d) above are not discharged by any of the parties, there shall be a rebuttable presumption that the damage has resulted from an error or a disruption having occurred within the sphere of responsibility of such party. Therefore, the agreement should contain a definition of what constitutes the sphere of responsibility of the sender of messages,[51] allowing the sender to exclude liability by proving it has complied with the obligations. Also, on this point it is interesting to note the provision of the German Model Agreement (art. 14.3.) allowing the sender to exclude liability when the error was obvious with reasonable care to the recipient and the damage could have been avoided.

Also, as mentioned above, it is common for the parties to use a value-added network provider to ensure an efficient passage of messages (as electronic mail processing systems: maintaining mailboxes and interconnecting with other providers). In case of intervention of a value-added network provider, a specific question arises: who will bear the fault of this party? Most EDI model agreements answer the question by allocating the risk in the following way: If one party uses the services of a value-added network to fulfil its tasks, rights and obligations, that party is liable to the other party for the actions and omissions of the value-added network to the same extent as it would have been for its own acts and omissions. If both parties enlist the services of the same value-added network, the originating party is responsible for the acts of the shared provider where that party initiates the final action with respect to any document. Of course, this provision will not affect the right to assert claims against the providers which remain applicable.

g. *On the Need for Having a Data Log or Storage*. Both parties should be required to record all messages in their entirety, chronologically, in an identifiable manner, protected from modification, manipulation, deletion and from being electronically written over. It must be ensured that the contents of all messages can at all times be made readable upon appropriate notice.

Periods of storage for electronic documents and electronic certificates shall be governed by the relevant prevailing national law of the parties.

The parties should obligate themselves to address messages conforming to the administrative and formatting requirements of the secure health care consortium.

Finally, as regards disputes, the parties should designate as arbitrator a health care consortium representative.

6. Conclusion

Digital signatures, trusted third parties services and cryptography are technical tools that will provide integrity, authenticity and confidentiality of electronic messages. Health care professionals willing to adopt a secure health telematic system (which provides integrity, authenticity and confidentiality) to carry out medical activities are forced to enter contracts with providers of security services, and in particular, with registration-certification authorities, with value-added services for secure communications, and with network providers. Nevertheless, because the customers will not likely have the power to negotiate contractual provisions which, in our view, would make sure an appropriate balance of obligations and duties between the providers of security services and the subscribers, and because contractual solutions by themselves have the disadvantage of binding only the parties who have signed the contract, it will be necessary to enact new law providing appropriate protection for the users.

The above statement would apply especially to the responsibility of registration and certification authorities. The registration authority should be responsible if it fails properly to identify the subscriber's identity under the criteria of "reasonable care". Also, the certification authority should be responsible under the criteria of reasonable care in the case it fails to bind the public key to the right owner, and in those cases where it fails to publish a revoked certificate. Nevertheless, because the burden of proving the lack of reasonable care would be too difficult to meet for a customer, we think that the burden of proof should be reversed.

Concerning who should act as registration and certification authority, in our view, it should be avoided to attribute this competence indiscriminately to a specific body (as chambers of physicians). To the contrary, regulating conditions to be fulfilled for those interested in carrying out TTP functions would lead to a regime allowing the establishment of competing TTP's according to marked needs.

Therefore, we think that it should be enacted a legal framework regulating TTP services, able to offer trust to users and courts, and establishing criteria under which TTP's would operate. This regulation should be combined with contractual agreements between the TTP's and subscribers of these services.

Value-added service providers could be employed by health care professionals for securing communications . In such cases, the health care actors should agree upon which services they would like to apply for in previous agreements (e.g., providing acknowledgement of receipt) and under which circumstances (e.g., they could agree on using the value-added acknowledgement of receipt only when the intended receiver fails to send it on his own).

Concerning network providers, in our view, the three following provisions should be considered for policy makers or eventually when drafting contracts between the network providers and subscribers (if they have any chance to negotiate): 1. The acceptance of liability for negligence instead of excluding all kind of liability; 2. The reversing of the onus probandi, which means that the subscribers would not need to prove the network provider's fault; 3. Definition of an entity responsible for the entire network.

Finally, regardless of the existence of a law regulating these issues, health care subscribers will have to enter contracts between them, regulating legal and technical aspects concerning how they will operate electronically.

Acknowledgement

Part of the research work has been carried out as part of the "Human Capital and Mobility" programme of the European Community which is financed by the Commission.

The authors want to acknowledge José Luis Ferrer Gomila, professor of telecommunications of the Balearic Islands' University for his help in the technical issues and Thomas C. Vinje, managing partner of Morrison & Foerster, for his valuable comments.

Notes

1. *Revolution in the Wings* (1993) Hospitals & Health Networks, June 20: 42–44; *Inching toward EDI: Experts Look at Obstacles* (1992) Hospitals, December 22: 42–43.
   As an example of the economic importance of Health care, below we reproduce a paragraph of The Global Internet Project's White Paper *"The Emergence of a Networked World"*, www.gip.org,: "Health Care in the United States alone is a $ 1 trillion industry representing 14 percent of gross domestic product and growing at 10 percent a year. It is already bigger than America's automobile, steel and transportation industries combined. At its present rate of expansion – and given its high wage, labour intensive natures and its modern dependence on expensive research and technology – American health care will be a $2 trillion industry by the year 2000".
2. Bialorucki, T. and Blaine, M. (1992) Protecting patient confidentiality in the pursuit of the ultimate computerised information system, *Journal of Nursing Care Quality*, N° 7: 53-56.
3. Nicolas, F. (1988) *Normas Comunes para las Empresas*, Bruselas-Luxemburgo.
4. EUROINFO TECH (1995) Thursday 16 November, Number 0113.
5. See: U.S., Congress, Office of Technology Assessment (1993) *Protecting Privacy in Computerised Medical Information*, OTA-TCT-576, Washington, DC: U.S. Government Printing Office and Smuckler, R. (1994) Health care and the Information Highway, Access and Privacy, *Canadian Medical Informatics*, Vol. 1, N° 2: 40-45.
6. A comparative analysis of different legal systems shows that contract law rarely requires a written document (with a hand-written signature) as a prerequisite for validity or enforceability of contracts. In those cases where contract law does have such a requirement, it applies to a kind of contract which does not belong typically to health care activity. An example can be found in what is referred to under civil law as "real contracts" (real property, marital acts), which obviously have nothing to do with the health care scenario. Another case where the law does require written documents with hand-written signatures is in consumer contracts, which, because health care activities do not fall into this category, will not apply to a health care scenario. Therefore, this requirement does not constitute a problem for the health care sector. See, Julià-Barceló, R. (1997) *Introduction to the legal acceptance of digital documents and signatures and liability of trusted third parties* (TRUSTHEALTH 1 Project HC 1051) and Julià-Barceló, R. Louveaux, S and Poullet, Y. (1997) *Legal aspects of Health Care Telematics. First Proposal for Actions in the Legal Area* (TRUSTHEALTH 1 Project HC 1051). These reports have been prepared under the TRUSTHEALTH and SIREN Projects, financed by D.G. XIII.
7. The issuance by a physician of a medical prescription could fall under the kind of administrative acts that the law requires to be in a written document, most of the times standardised.
8. Bialorucki, T. and Blaine, M. (1992) Protecting patient confidentiality in the pursuit of the ultimate computerised information system, *Journal of Nursing Care Quality*, N° 7: 53-56.
9. Article 9.2. provides: "In order to ensure the confidentiality, integrity and accuracy of processed data as well as the protection of patients, appropriate technical measures should be taken: a. to prevent any unauthorised access to the information's systems used to process personal data; b. in order to prevent the contents of date can be read, copied modified or redirected by a non-authorised person; c. to prevent the introduction of non-authorised date in the system, as well as all kind of diffusion, modification or destruction of personal data . . .". (non official translation).

10. Katus, S. (1992) Three types of EDI contracts, *Law, Computers and Artificial Intelligence*, Vol. 1, Number 3: 259–273, defines the network agreements as follows: "Agreements that regulates the rights and obligations of users and intermediaries with regard to technical requirements and legal issues, to ensure an efficient passage of EDI messages in an atmosphere of legal security".
11. The most popular algorithms for public key cryptosystems is the Rivest, Shamir, Adleman (RSA) encryption technique and DSS which in 1994 has been adopted by the national Institute of Standard Technology, National Institute of Standards and Technology (1994) Federal Register Vol 59, N° 96, Notices.
12. U.S. Congress, Office of Technology Assessment (1995) Issue Update on Information Security and Privacy in Network Environments, Washington, D.C.
13. In closed networks the authentication of the identity of a sender can be achieved *between trading partners* through bilateral agreements where the parties exchange encryption keys between themselves and provide the necessary technical set-up for their communication.
14. As we will see below, this is a name given by the registration (or more precisely the naming authority) for the purpose of guaranteeing the uniqueness of every name issued.
15. The validity period of the digital signature itself has to be limited because mathematical and technological advances make it possible to crack keys of the originally chosen limited length. See Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E. and Wiener, M. (1996) *Minimal key lengths for symmetric ciphers to provide adequate commercial security*, file///C/WINDOWS/TEMP/cryptologists.html
16. Froomklin, M. (1996) The Essential Role of the Trusted Third Parties in Electronic Commerce, *75 Oregon Law Review*, 49, p. 63 classify those certificates as "authorising certificates".
17. The actor in charge of providing such a service is known as a "registration authority".
18. Certification authority is the name received by the actor offering certification functions.
19. We want to point out that an important issue is the transmission or management of keys for signature and confidentiality. It applies also to the transmission of certificates: What the certification authority does with the certificate (in order to forward it to the key holder) depends on the services the certification authority offers and this choice will affect the legal regime of the certification authority (e.g., liabilities).
20. E.g., Belsign: Belgian Chamber of Commerce acts as registration authority and Belsign as certification authority. In order to limit the scope of the article, we will not analyse the contractual framework between the registration authority and certification authority.
21. This function has been foreseen in the report entitled TEDIS – Service infrastructure for EDI Security (1993). A report compiled by the National Computing Centre, Manchester, and by the art. 8 (3) of the Basic Electronic Data Interchange (EDI) Agreement.
22. E.g., Infosec provides the following example of using of this functions: An user A signs a message in 1993 and sends it to B. Then it turns that his private key has been compromised in 1994. A cancels his certificate. B would be in a better position if the had sent A's message to a Time stamping TTP who will has time stamped and signed the message produced by A which will proof that it was issued by A in a certain period of time before the compromise of the private key.
23. See: TEDIS – *Security in Open Environments*, (1994), Luxembourg.
24. Baker, S., *Decoding the OECD's Guidelines for Cryptography Policy*, early version of an article that will appear in the Fall issue of the *International Lawyer* found (http://www.steptoe.com/comment.htm). Baker's interpretation of this principle defends that the adherence to the obligations assumed under the OECD's 1980 Guidelines on privacy is sufficient to fulfil the privacy obligations created by this principle.
25. In fact, experts recognise a good strategy for technology and infrastructures should integrate solutions for confidentiality with the solutions for secure authentication of user identity and digital signatures (mainly through the use of digital signatures to interchange private/session keys). Klein, G., (1996) *The proposed Encryption Strategy for the English National Health Care in a European perspective, Sweden.*

26. In this paper we do not analyse policy making aspects concerning government regulations about storing secrete keys with a trusted third party (known as key escrow or key recovery). For more information see e.g.: Foomkin, M., (1996) It came from planet clipper: the battle over cryptographic key "escrow", *The University of Chicago Legal Forum*, Vol. 15: 14–74; Kuner, C., (1996), Legal aspects of encryption in the internet, *International Business Lawyer*, Vol 24, N° 4: 186–191; Kirby, J.M. (1997) Cryptography policy, *Computer Law & Security Report*, Vol. 13 N° 3: 182–186; Kuner, C. (1997) Criptography regulation in Germany: Present and Future, *Computer & Telecommunications Law Review*, Vol. 3, Issue 3: 116–118.
27. http://www.ispo.cec.be/Ecommerce
28. http://wwwoecd.org/dsto/iccp/crypto-e.html
29. (A/CN.9/ 437 12 March 1997).
30. E.g., Utah Digital Signature Act (Supp. 1996), Hawaii (1995), California (Deering 1996), New York, Arizona, Washington, Virginia, Wyoming, Florida, South Carolina Digital Signature Act (draft bill). Tinnes, C. (1997) The Proposed Digital Signature Act of 1997, *South Carolina Law Review*, 48: 172–185.
31. Wyrough, W.; Klein, R. (1996) The Electronic Signature Act of 1996: Breaking down barriers to widespread electronic commerce in Florida, *Florida State University Law Review*, Vol 24: 407–437.
32. As Andersen, M. (1994) The Danish Teletrust-Initiative, *The EDI Law Review*, Vol 1, N° 1: 50–51, says by determining that a certificate is a service, the EC Product Liability Directive (85/374/EEC) could be applicable. It could also be applicable analogically. Under art. 15 of the Directive the producer of a defective product is not liable under the strict product liability regime, if he can prove that the state of scientific and technical knowledge at the time he put the product into circulation was not such to enable the defect to be discovered. In our view this would lead to negative consequences for the user of digital certificates because he will bear the risk of mistakes suffered by the registration and certification authority.
33. See Gainer, R. (1997) Allocating the risk of loss for bank card fraud on the internet, *The John Marshall Journal of Computer & Information Law*, Vol. XV, N° 1: 39–49.
34. This approach has been taken in the EFT Act (concerning debits cards) and Federal Consumer Protection Act (concerning credits cards). For a more detailed study, see: Gainer, R. (1996) Allocating the risk of loss for bank card fraud on the internet, *The John Marshall Journal of Computer & Information Law*, Vol XV, N° 1: 39–49.
35. The use of digital signatures within digital certificates which require the key holder to keep secret the private key and therefore, oblige him not to allow his private key to fall into the hands of somebody else, has been criticized by some authors arguing that this concentrates the risk in the private key holder. See: Wright, B. (1997) Eggs in baskets: distributing the risks of electronic signatures, *The John Marshall Journal of Computer & Information Law*, Vol. XV, N° 2: 189–201.
36. See Rapport du Groupe de Travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 18-28 février 1997), A/CN.9/437.
37. This function is offered by Veridial, See: TEDIS – Service infrastructure for EDI Security (1993) A report compiled by the National Computing Centre, Manchester.
38. However, by taking this approach the recipient bears the risk of a malfunction of the system (between the mailbox and his computer) disabling him from reading the message or even realising its existence.
39. For more details about agreements on this provision, see: Alcover Garau, G. (1994) La firma electrónica como medio de prueba (valoración jurídica de los criptosistemas de claves asimétricas), *Cuadernos de Derecho y Comercio*, N° 13: 11–41.
40. Value-added service providers will make available to users who wish to benefit from others value-added services. Examples of such network providers IBM, Infonet, INS, Geisco. For the purposes of this article we will assume that value-added network providers are used instead of public telecommunications operators. Also we will exclude from our study the

analysis of the contractual relationship between the telecommunications operator and the value-added service provider. Nevertheless, generally speaking, up to now, most countries telecommunications organisations as public services carried out by the State, have been subjected by law to specific rules, by virtue of the special or exclusive rights conferred on the organisations, excluding or diminishing their liability.

41. TEDIS – *The liability of electronic data interchange operators*, (1991) CRID, Brussels.
42. American precedents have applied in the field of E.F.T. the theory of "transmitting cost avoider" which means that the one who has best position in the transmission chain to avoid damages must assume full liability for an incident. See, for a more detailed study: Thunis, X. (1996) *Responsabilité du banquier et automatisation des paiements*, Travaux de la Faculté de Droit de Namur, No 19, Presses Universitaires de Namur, Namur.
43. Baker, S., *Decoding the OECD's Guidelines for Cryptography Policy*, found in internet: http://www.steptoe.com/comment.htm, says that the principle 7 of OECD's Guidelines which deals with liability suggest to the governments enacting rules that discourage negligence in the handling of private keys by imposing liability rules under negligent behaviour.
44. Commission Recommendation of 19 October 1994 relating to the Legal Aspects of Electronic Data Interchange (J.O. N° L338 du 28.12.94).
45. American Bar Association (1990) Model Electronic Data Interchange Trading Partner Agreement, published in *The Business Lawyer*, Vol. 45: 1717–1748; German Basic Electronic Data Interchange Agreement published in *The EDI Law Review*, 1996, N° 3: 53–62, UNCITRAL Model Law on Electronic Commerce, etc.
46. For more details see: Blechschmidt, R. (1996) The German Basic Electronic Data Interchange Agreement versus the European Model EDI Agreement: Some Reflections on German Law, *The EDI Law Review*, N° 3: 107–124.
47. (1) A message shall be deemed to have been received by the recipient by means of Data Transmission when received by the recipients Communications Equipment and when an automatic confirmation of receipt from the recipients Communications Equipment has been received by the senders Communications Equipment. (2) A Message shall be deemed to have reached the recipient by means of Data Retrieval when it has been made available for retrieval in the section of the senders Communications Equipment designated for this purpose and has been retrieved by the recipient there, and when an automatic confirmation of retrieval from the recipient's Communications Equipment has been received by the senders Communications Equipment. (3) If value added networks have been commissioned, a Message shall be deemed to have been received by the recipient if, by means of Data Transmission, the Message has entered the recipient's value added network mailbox and a confirmation from that value added network has been received by the sender's Communications Equipment. (4) If a message arrives outside Business Hours, it shall be deemed to have been received by the recipient at the start of business hours on the next Business Day. (5) In addition to the confirmation referred to in paras 1 and 2, the sender may, at the time of any Data Transmission, request a separate acknowledgement retrieval from the recipient, and the recipient may, when retrieving data, request a separate acknowledgement of retrieval from the sender at the time of any Data Retrieval. The separate acknowledgement must have been received by the sender/recipient within Business Hours on the next Business Day following the transmission or retrieval of data. A Message requiring acknowledgement in accordance with this paragraph shall only be deemed effectively transmitted or effectively retrieved if this acknowledgement is given, without prejudice to the times of receipt stipulated in paras 1, 2 and 4.
48. Nevertheless, this provision might encounter a validity problem: agreements about evidence are not always accepted under some European laws (e.g., German law). See Hoeren, T. (1994) Evidential Problems of Electronic Document – The Need for EC Policies, *The EDI Law Review*, Vol. 1, N° 2: 77–82.
49. See point 3.2 and 3.3 above.

50. Art. 2.4. of American Bar Association, Model Electronic Data Interchange Trading Partner Agreement; Art 13 of the German Basic Electronic Data Interchange Agreement, art 6.3. of the European EDI Model Agreement.
51. The German Model foresees the following: "The sphere of responsibility of the sender of Messages shall cover its Communications Equipment, its Communications Security and the period of time until receipt of the Message. The sphere of responsibility of the recipient of Messages shall cover its Communications Equipment, its Communications Security and the period of time following receipt of the Message". Also: (3) "Each party shall bear the costs of identifying errors which are located or arise within its sphere of responsibility. If an error occurs which cannot definitely be assigned to either party's sphere of responsibility, the party most likely to have been in a position to avoid the error shall bear the entire costs of the search for errors. If this can not be clarified, each party shall bear one half the costs of identifying the error". (4) "The liability pursuant to para 1 shall cover all personal injury, damage to property and pecuniary loss including the costs of identifying errors, regardless of which party has borne the costs in the first place. Compensation for damage to property and pecuniary loss shall be limited to a maximum amount of . . . of the damage incurred by the other party as a result of reliance on the authenticity, accuracy or completeness of the Message. Liability for damages shall arise only so in far as the other party was unaware that the message was not authentic, accurate or complete and also could not, with reasonable care, have recognised this fact The maximum amount for intangible damage is . . . ".